BLOOD HURST & O'REARDON, LLP
LESLIE E. HURST (178432)
PAULA R. BROWN (254142)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
lhurst@bholaw.com
pbrown@bholaw.com

Attorneys for Plaintiff

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA – WESTERN DIVISION

SEAN DEMARCO and DAVID JOHNSON III, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. MARRIOTT INTERNATIONAL, INC., Defendant.	Case No. 2:18-cv-10490 **CLASS ACTION** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Sean DeMarco and David Johnson III ("Plaintiffs"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to themselves and on information and belief as to all other matters, bring this action against Defendant Marriott International, Inc. ("Marriott"), and respectfully state the following:

NATURE OF THE CASE

1. On November 30, 2018, Marriott announced one of the largest data breaches in history. The Marriott data breach, which was not announced until at least four years after it first began, involves some of the most sensitive and private information from approximately 500 million consumers whose information was on Marriott's Starwood guest reservation database (the "Data Breach"). According to Marriott, there has been "unauthorized access to the Starwood network since 2014," through which "an unauthorized party had copied and encrypted information, and took steps towards removing it." Marriott believes the compromised guest reservation database "contains information on up to approximately 500 million guests who made a reservation at a Starwood property." Four years after the Data Breach first began, Marriott finally revealed the information accessed in the Data Breach includes names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest ("SPG") account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, as well as payment card numbers, and payment card expiration dates.

2. Marriott admits that hackers gained access to and compromised the confidential and sensitive, personal and private information of anyone who made a reservation on or before September 10, 2018, for any Starwood property. These Starwood properties include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection,

Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton Hotels, and Starwood-branded timeshare properties (*e.g.*, Sheraton Vacation Club and Westin Vacation Club). According to Marriott, "[r]egardless of whether you are an SPG member, if you made a reservation on or before September 10, 2018 for a Starwood property, information you provided may have been involved."

3. Marriott is the world's largest hotel chain. As part of its business, Marriott collects and organizes personal private information about consumers, including Plaintiffs and other Class members. Plaintiffs and the other Class members reasonably expect and believe that Marriott will take appropriate measures to protect their personally identifiable information ("PII"). Indeed, Marriott's CEO admitted it "fell short of what our guests deserve and what we expect of ourselves." Likewise, in its 2017 Annual Report, Marriott also recognized "[o]ur guests … have a high expectation that we … will adequately protect their personal information."

4. Marriott's cybersecurity measures were so deficient that it took four years for it to discover that criminal hackers had gained access to Plaintiffs' and Class members' PII.

5. Marriott owed a legal duty to Plaintiffs and the other Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard the personal information stored on its network. Marriott breached that duty by failing to design and implement appropriate firewalls and computer systems, failing to properly and adequately encrypt data, and unnecessarily storing and retaining Plaintiffs' and the other Class members' personal information on its inadequately protected network.

6. As the result of Marriott's inadequate cybersecurity, the Data Breach occurred and Plaintiffs' and the other Class members' PII was compromised and stolen, placing them at an increased risk of fraud and identity

theft, and causing direct financial expenses associated with credit monitoring, replacement of passports, compromised credit, debit and bank card numbers, and other measures needed to protect against fraud arising from the Data Breach.

7. This action seeks to remedy these failings. Plaintiffs bring this action on behalf of themselves and persons whose personal or financial information was disclosed as a result of the data breach first disclosed by Marriott on or about November 30, 2018.

8. Plaintiffs seek, for themselves and the Class, injunctive relief, actual and other economic damages, consequential damages, nominal damages or statutory damages, punitive damages, and attorneys' fees, litigation expenses and costs of suit.

VENUE AND JURISDICTION

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different from Defendant.

10. This Court has personal jurisdiction over Marriott because Marriott is authorized to conduct business in California and does, in fact, conduct business in California. Marriott therefore has sufficient minimum contacts with the state to render exercise of jurisdiction by this Court in compliance with traditional notions of fair play and substantial justice.

11. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because Marriott regularly conducts business in this district, unlawful acts or omissions are alleged to have occurred in this district, and Marriott is subject to personal jurisdiction in this district.

PARTIES

12. Plaintiff Sean DeMarco resides in Torrance, California. Believing that Marriott would safeguard his PII, on more than one occasion Mr. DeMarco provided Marriott with his confidential and highly sensitive personal and private information in connection with making reservations at Marriott's Starwood hotels. This included information such as: first and last name; home telephone number; e-mail address; current and former mailing address; and credit card number and expiration date.

13. On December 7, 2018, Mr. DeMarco, received an email from Marriott confirming that his sensitive PII has been compromised and stolen as a result of the Data Breach and Marriott's unlawful conduct alleged herein. As a direct and proximate result of Marriott's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud[1] inflicted on Plaintiff by one or more unauthorized third parties, Plaintiff also has suffered (and will continue to suffer) economic damages and other injury and harm in the form of the deprivation of the value of his PII, for which there is a well-established national and international market. PII is a valuable property right. Faced with the choice of having his PII disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without his authorization versus selling his PII on the black market and receiving the compensation himself, Plaintiff would choose the latter. Plaintiff – not data thieves – should have the exclusive right to monetize his PII. Marriott's wrongful

[1] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services, including medical services).

actions, inaction and omissions, and the resulting Data Breach, deprived him of this right.

14. As a further direct and proximate result of Marriott's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud inflicted by one or more unauthorized third parties, Mr. DeMarco has suffered (and will continue to suffer) other economic damages and injury and harm, including: (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud; (ii) invasion of privacy; (iii) breach of the confidentiality of his PII; (iv) deprivation of the value of his PII, for which there is a well-established national and international market; and/or (v) the financial and/or temporal cost of monitoring his credit, monitoring his financial accounts, and mitigating his damages – for which he is entitled to compensation.

15. Plaintiff David Johnson III resides in Port Richey, Florida. Believing that Marriott would safeguard his PII, on more than one occasion Mr. Johnson provided Marriott with his confidential and highly sensitive personal and private information in connection with making reservations at Marriott's Starwood hotels. This included information such as: first and last name; home telephone number; e-mail address; current and former mailing address; and credit card number and expiration date.

16. On December 6, 2018, Mr. Johnson, received an email from Marriott confirming that his sensitive PII has been compromised and stolen as a result of the Data Breach and Marriott's unlawful conduct alleged herein. As a direct and proximate result of Marriott's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud[2] inflicted on Plaintiff by one or more unauthorized third parties, Plaintiff

[2] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing

also has suffered (and will continue to suffer) economic damages and other injury and harm in the form of the deprivation of the value of his PII, for which there is a well-established national and international market. PII is a valuable property right. Faced with the choice of having his PII disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without his authorization versus selling his PII on the black market and receiving the compensation himself, Plaintiff would choose the latter. Plaintiff – not data thieves – should have the exclusive right to monetize his PII. Marriott's wrongful actions, inaction and omissions, and the resulting Data Breach, deprived him of this right.

17. As a further direct and proximate result of Marriott's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud inflicted by one or more unauthorized third parties, Mr. Johnson has suffered (and will continue to suffer) other economic damages and injury and harm, including: (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud; (ii) invasion of privacy; (iii) breach of the confidentiality of his PII; (iv) deprivation of the value of his PII, for which there is a well-established national and international market; and/or (v) the financial and/or temporal cost of monitoring his credit, monitoring his financial accounts, and mitigating his damages – for which he is entitled to compensation.

18. Defendant Marriott, International, Inc. is a Delaware corporation, with its headquarters and principal place of business located at 10400 Fernwood Road, Bethesda, Maryland 20817.

various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services, including medical services).

19. Marriott is the largest hotel chain in the world. Marriott has an approximate 15% share of the U.S. hotel market. By the end of 2017, Marriott had more than 6,500 properties (over 1.2 million rooms) in 30 hotel brands across 127 countries and territories. On September 23, 2016, Marriott completed the acquisition of Starwood Hotels & Resorts Worldwide, LLC, formerly known as Starwood Hotels & Resorts Worldwide, Inc. ("Starwood"), after which Starwood became an indirect wholly-owned subsidiary of Marriott. Starwood's reservation services include communicating reservations and their details to its hotels that individuals make directly with Starwood online, through Starwood's mobile apps, telephone call centers, and intermediaries like travel agents, and Internet travel websites. Using the massive Starwood guest reservation database, Marriott directly collects and maintains guests' PII for all Starwood properties.

FACTUAL ALLEGATIONS

Personal Identification Information Is a Valuable Property Right

20. At a Federal Trade Commission ("FTC") public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's PII:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy.
>
> Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[3]

21. Though Commissioner Swindle's remarks are more than a decade old, their pertinence has increased over time, as PII functions as a "new form of

[3] Federal Trade Commission, *The Information Marketplace: Merging and Exchanging Consumer Data*, *Conference and Workshop*, *Washington D.C.*, 28 (March 13, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

currency" that supports a $26 billion per year online advertising industry in the United States.[4]

22. The FTC has also recognized that PII is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

23. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent, consumers will make a profit from the surrender of their PI.[6] This business has created a new market for the sale and purchase of this valuable data.[7]

24. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed,

---

[4] *See* J. Angwin and W. Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, Feb. 28, 2001, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

[5] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[6] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times, July 16, 2010, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html?_r=0.

[7] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal, Feb. 28, 2011, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

25. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII – the very injury at issue here – between $11.33 and $16.58 per website.[9]

26. The United States Government Accountability Office noted in a June, 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[10] As the GAO Report states, this type of identity theft is the most harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

27. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name."

28. According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and

[8] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* http://www.guanotronic.com/~serge/papers/isr10.pdf.

[9] II–Horn, Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.321.6125&rep=rep1&type=pdf (emphasis added).

[10] *See* http:///www.gao.gov/new.items/d07737.pdf.

credit record.[11] Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12]

29. Data breaches involving passport numbers can be particularly damaging. Passport information can provide thieves with a second form of ID typically required for opening accounts or proving residence. Fake passports on the black market reportedly sell for $4,000 or more.[13]

30. According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it." Some of the ways identity thieves can use PII include:[14]

- Open a new credit card of loan.
- Change a billing address so you will no longer receive the bills.
- Open new utilities in your name.
- Obtain a mobile phone.
- Open a bank account and write bad checks.
- Use your debit card number to withdraw funds.
- Obtain a new driver's license or ID.
- Use your information in the event of an arrest or court action.

---

[11] *See* FTC Identity Theft Website: www.ftc.gov/bcp/edu/microsites/idtheft /consumers /about-identity-theft.html.

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[13] *See* https://www.popsci.com/passport-number-hacked-marriott

[14] *See* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/

31. Another one of the various ways thieves can use the PII accessed during the Marriott Data Breach is to piece together Class member's travel history and determine their vulnerabilities. For instance, to obtain your international travel history, an online tool maintained by the Department of Homeland Security requires your full name, birthday, and passport number – all of which were part of the Marriott Data Breach. *See* https://i94.cbp.dhs.gov/I94/#/history-search#section.

32. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

33. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[15]

34. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[16] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious

---

[15] *See* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[16] *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (citations omitted).

risk to reward analysis illustrates beyond doubt that PII has considerable market value.

35. Companies, in fact, also recognize PII and other sensitive information as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[17]

36. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information obtained in the Marriott Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[18]

37. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived

[17] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

[18] http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/

that consumer of the full monetary value of the consumer's transaction with the company.

38. It is within this context that Plaintiffs and half a billion consumers must now live with the knowledge that their personal information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Marriott Failed to Timely Disclose the Data Breach

39. On November 30, 2018, Marriott announced the massive Data Breach through which criminals gained access to a database containing sensitive personal data for a staggering 500 million Starwood hotel guests, including names, birth dates, addresses, passport numbers, credit card numbers, and other PII.

40. According to Marriott, the hackers had access to the aforementioned sensitive, personal information of approximately 500 million persons from at least 2014 until September 8, 2018, when the intrusion was discovered.

41. While Marriott learned of the Data Breach on or before September 8, 2018, it waited months before informing the public. As of filing this complaint, it is unclear whether all Class members affected by the Data Breach have been personally notified by Marriott.

42. The email notification that some Class members received was misleading as well. The emails that have been sent are from "email-marriott.com," a website "registered to a third-party firm, CSC, on behalf of the hotel chain giant."[19] This domain does not load or have an HTTPS identifying certificate. It is known that phishing scammers use data breaches as an

[19] Zack Whittaker, *Marriott's breach response is so bad, security experts are filling in the gaps – at their own expense*, Tech Crunch, Dec. 3, 2018, https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/

opportunity to gain access to PII, but Marriott insisted on using the problematic email-marriott.com domain. For example, security expert Troy Hunt recently registered "email-mariott.com" which could have been used by scammers.[20] The use of this ambiguous email address only adds to the confusion.

Marriott's Belated Description of the Data Breach Is Inadequate and Misleading

43. As of December 13, 2018, more than three months since Marriott discovered the Data Breach, it still had not sent all Class members notice that their sensitive PII was compromised and stolen. Instead, as described herein, the belated public statements Marriott did make about the Data Breach are misleading, incomplete and fail to provide consumers with basic, important information about the scope and breadth of the stolen PII, and even whether their sensitive PII was accessed and stolen in the first place.

44. On November 30, 2018, Marriott issued a press release that hackers gained access to the most sensitive, private data of approximately 500 million Starwood hotel guests. The release is materially misleading and does not disclose to consumers the full scope of the ongoing threat.

45. On the same day as the press release, Marriott set up a website for consumers to "answer questions you may have about this incident." The website, info.starwoodhotels.com, which links consumers to answers.kroll.com is misleading and does not provide material information to consumers. It merely repeats the misleading information in the press release. For example, the website does not inform consumers of the potential consequences of their stolen information or describe sufficient steps to take to protect their PII. Instead, it simply instructs some consumers to sign up for "WebWatcher," an insufficient cybersecurity tool, and on the very bottom of the page Marriott lists "other steps" for consumers to take like monitoring their SPG account, changing passwords

[20] *Id.*

and reviewing payment card accounts. However, Justin Brookman, director of consumer privacy and technology policy for Consumer Reports, states that internet web monitoring products such as WebWatcher "can offer a false sense of security and aren't particularly effective at protecting your data."[21] The WebWatcher product does not protect consumer information it merely alerts them that "the crooks already have it and you can't get it back from them."[22]

46. In an article *Why Marriott's ID Theft Protection May Not Be Enough*, Consumer Reports explains that there are much more useful steps to take than described by Marriott. Some of these include examining homeowners' insurance, employee benefit packages and union memberships which often have more robust ID theft insurance policies. Marriott does not mention monitoring credit reports, a service not covered by the WebWatcher product, or freezing your credit which is the "most effective way to preemptively guard against criminals opening accounts in your name."[23] Nor does it mention "contacting the big three credit bureaus online: Experian, Equifax and TransUnion. Freezing your information at just one won't offer the fullest protection possible."[24]

47. Marriott's Data Breach press release and website also failed to explain the breadth of the Data Breach and the potential threat that consumers' face as a result of the sensitive PII being in the hands of criminals. For example, there are no specifics about how the breach occurred or why consumer PII was not properly safeguarded and protected. Although Marriott told Consumer Reports that "it's working on a solution to help guests who want to change their

---

[21] Octavio Blanco, *Why Marriott's ID Theft Protection May Not Be Enough*, Consumer Reports (Dec. 7, 2018), https://www.consumerreports.org/identity-theft/why-marriotts-id-theft-protection-may-not-be-enough/

[22] *Id.*

[23] *Id.*

[24] *Id.*

passports[,]" there is no mention of this in its press release or on its website.[25] Marriott's website also does not reference that renewing your passport will change the passport number, which is another useful tool in preventing unauthorized use of PII.

48. Many affected consumers will not see Marriott's press release or check if they were potentially impacted by visiting Marriott's website. Marriott could have sent text messages, like J.P. Morgan Chase and other banks use to instantly notify customer of a fraud alert of breach of their secured account, but instead chose to only issue a press release, set up a website, and send delayed emails.

49. Thus, Marriott's press release, its website for consumers to check for potential impact, and its other public statements about the Data Breach are misleading, do not adequately inform consumers about the steps that should be taken to protect against identity theft, and do not provide sufficient details about the scope and breadth of the Data Breach, including what specific information of theirs was accessed and stolen.

Marriott's Offer of Limited Information Monitoring Is Inadequate and May Compromise Consumers' Rights

50. Marriott's Data Breach notices also squarely place the burden on Plaintiffs and Class members, rather than Marriott, to protect themselves and attempt to mitigate their data breach damages. Marriott instructed its customers to review their SPG account for suspicious activity, change account passwords, review credit and debit card statements, and "[b]e vigilant against third parties attempting to gather information by deception."

51. Marriott's Data Breach notice states that Marriott will provide one year of Kroll's "WebWatcher" information monitoring to U.S. consumers. According to Marriott, "WebWatcher monitors internet sites where personal

[25] *Id.*

information is shared and generates an alert if evidence of your personal information is found." WebWatcher enrollment also provides limited reimbursement for expenses incurred with one identity theft incident, and the ability to consult with a fraud specialist. One year of WebWatcher monitoring however, is inadequate and requires affected customers to spend additional time and resources to obtain coverage. To make matters worse, unbeknownst to the reasonable consumer, to sign up for WebWatcher, Kroll purports to bind them to its "Terms and Conditions", which includes a mandatory arbitration provision, jury waiver, and class action waiver.

52. The one-year information monitoring offered by Marriott also does not provide comprehensive protection to the affected customers. Marriott does not disclose this important fact. For example, the limited one-year offer does not account for the fact that a person whose personal information has been compromised may not see any signs of identity theft for several years.

Hotels, Including Marriott's Starwood Hotels, Have a Long History of Data Breach Incidents

53. Hoteliers, including Marriott, are known to be and have been particularly vulnerable to data breaches. In the past decade, highly-publicized data breach events have occurred at numerous hotel chains, including Hilton, Hyatt, Starwood, Mandarin Oriental, Wyndham, Kimpton, Omni, Four Seasons, Hard Rock, Loews, Trump Hotels, and InterContinental locations. Despite the large and growing number of data breach events at hotel chains across the country and worldwide, Marriott failed to adequately safeguard Plaintiffs and Class members' sensitive PII.

54. In connection with three breaches between 2008 and 2010, hackers gained access to Wyndham Worldwide's systems. The hackers accessed data on more than 619,000 accounts, and the breaches resulted in an estimated $10.6 million in fraudulent charges.

55. In 2015, two separate breaches resulted in the exposure of more than 350,000 credit cards used by Hilton Worldwide guests.

56. In March 2015, Mandarin Oriental disclosed that the credit card systems in at least 20 of its hotels had been hacked.

57. In November 2015, Starwood announced a malware-driven credit card data breach. According to Starwood, point-of-sale systems at more than 70 Starwood properties in North America were breached during the attack that occurred between November 2014 and June 2015.

58. In December 2015, Starwood disclosed that hackers obtained credit and debit card information of customers from 54 of its hotels.

59. In 2016, Kimpton hotels announced that thieves had tapped guest data via its point-of-sale systems over a five-month period. Payment card data stolen during the Kimpton breach has been used to make unauthorized charges.

60. In 2016, Omni Hotels & Resorts revealed a malware breach involved customer credit and debit cards at 49 of the chain's 60 locations. That same year, Millenium Hotels & Resorts announced a breach at 14 of its properties.

61. In 2017, InterContinental Hotels Group announced that hackers compromised POS systems at more than 1,000 hotel properties.

62. In 2015 and again in 2017, Hyatt suffered data breaches through its POS systems as well. The former breach involved 250 Hyatt hotels worldwide.

63. In November 2018, Radisson announced that hackers gained access to information of certain Radisson Rewards members.

Marriott Failed to Honor Its Promises to Keep Sensitive Personal Information Confidential

64. In regulatory filings Marriott publicly acknowledges the importance of safeguarding its "customer data, including credit card numbers and other personal information in various information systems that we maintain" because

the "integrity and protection of that customer … data is critical to our business."[26] Marriott knew that Class members had "high expectations" that it would "adequately protect their personal information."[27]

65. In its 2008 Annual Report, Marriott disclosed that "[f]ailure to maintain the integrity of internal or customer data could result in faulty business decisions, damage of reputation and/or subject us to costs, fines or lawsuits. Our businesses require collection and retention of large volumes of internal and customer data, including credit card numbers and other personally identifiable information of our customers[.]"[28] Again, Marriott recognized that customers "have a high expectation that we will adequately protect their personal information[.]"

66. To this date, Marriot touts that it is "Privacy Shield Certified" and "recognizes that privacy is important" to consumers on its website, marriott.com. Marriott also promises to "use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information."

67. At all relevant times, Marriott designed and implemented its policies and procedures regarding the security of protected financial information and sensitive information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected financial information and other sensitive information.

68. Plaintiffs and Class members relied on Marriott to keep their sensitive information safeguarded and otherwise confidential.

---

[26] Marriott Form 10-Q for the quarter ended September 30, 2016.

[27] *Id.*

[28] Marriot 2008 Annual Report *available at* https://marriott.gcs-web.com/static-files/98c00f47-7670-450b-af25-2b9ab6259f9d

69. Marriott's wrongful actions, inaction, omissions, and want of ordinary care in failing to completely and accurately notify Plaintiffs and the Class about the Data Breach and corresponding unauthorized release and disclosure of their personal information was arbitrary, capricious and in derogation of Marriott's duties to Plaintiffs and the Class.

CLASS DEFINITION AND ALLEGATIONS

70. Plaintiffs bring this class action lawsuit on behalf of themselves and all other members of the Class (the "National Class") defined as follows:

> All persons in the United States whose personal or financial information was compromised as a result of the data breach first disclosed by Marriott on or about November 30, 2018.

71. In the alternative to the National Class, Plaintiffs seek certification of California and Florida Classes defined as follows:

> **California Class**
>
> All persons in California whose personal or financial information was compromised as a result of the data breach first disclosed by Marriott on or about November 30, 2018.
>
> **Florida Class**
>
> All persons in California whose personal or financial information was compromised as a result of the data breach first disclosed by Marriott on or about November 30, 2018.

72. The National Class, California Class, and Florida Class are collectively referred to as the Class.

73. Excluded from the Class are: (1) Marriott and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

74. **Numerosity.** While the exact number of Class members is unknown, Marriott has admitted the personal information, including names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers of approximately 500 million consumers was taken during the Data Breach. Plaintiffs therefore believe that the Class is so numerous that joinder of all members is impractical.

75. **Typicality.** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and the Class members were injured by the same wrongful acts, practices, and omissions committed by Marriott, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

76. **Commonality.** Common questions of law and fact exist as to all Class members and predominate over any individual questions. Such common questions include, but are not limited to:

(a) Whether Marriott has engaged in unlawful, unfair or fraudulent business acts or practices;

(b) Whether Marriott has engaged in the wrongful conduct alleged herein;

(c) Whether Marriott used reasonable or industry standard measures to protect Class members' personal and financial information;

(d) Whether Marriott adequately or properly segregated its network so as to protect personal customer data;

(e) Whether Marriott knew or should have known prior to the security breach that its network was susceptible to a potential data breach;

(f) Whether Marriott should have notified the Class that it failed to use reasonable and best practices, safeguards, and data security measures to protect customers' personal and financial information;

(g) Whether Marriott should have notified Class members that their personal and financial information would be at risk of unauthorized disclosure;

(h) Whether Marriott intentionally failed to disclose material information regarding its security measures, the risk of data interception, and the Data Breach;

(i) Whether Marriott's acts, omissions, and nondisclosures were intended to deceive Class members;

(j) Whether Marriott's conduct violated the laws alleged;

(k) Whether Plaintiffs and the Class members are entitled to restitution, disgorgement, and other equitable relief; and

(l) Whether Plaintiffs and the Class members are entitled to recover actual damages, statutory damages, and punitive damages.

77. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests which are adverse to or conflict with those of the Class members Plaintiffs seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

78. **Superiority.** A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class may be relatively small. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or

contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Negligence

79. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

80. During the course of conducting its business, Marriott collected consumer's PII. It was reasonably foreseeable that third parties would attempt to acquire such information given the risk and frequency of security breaches and highly publicized breaches elsewhere, including a December 2015 Starwood incident which was just prior to Marriott's purchase of Starwood where hackers obtained credit and debit card information of customers from 54 of its hotels.

81. In addition, Marriott had notice of a possible security breach due to the prior targeting of other hoteliers, large retailers and financial institutions by third parties seeking such information.

82. Consequently, Marriott as one of the largest hotel chains in the world, was entrusted with the sensitive PII of over 500 million consumers worldwide, was trusted by its customers and other consumers to safeguard their personal and private information, including sensitive financial data such as credit card numbers. Marriott had a special duty to exercise reasonable care to protect and secure the PII, so as to prevent its collection, theft, or misuse by third parties.

83. Marriott should have known to take precautions to secure consumers' PII, given its special duty.

84. Marriott likewise had a duty to exercise reasonable care under the circumstances to prevent any breach of security that would result in the loss,

disclosure or compromise of the personal and financial information of Plaintiffs and the Class, given its prior knowledge of security breaches.

85. Marriott also had a duty to exercise reasonable care under the circumstances to detect any breach of security that would result in the loss, disclosure or compromise of the personal and financial information of Plaintiffs and the Class.

86. Once a security breach was detected, Marriott had a duty to exercise reasonable care under the circumstances to notify affected persons in order to minimize potential damage to Plaintiffs and the Class due to the loss, disclosure or compromise of their personal and financial information.

87. Marriott breached its duty of care by failing to adequately secure and protect Plaintiffs' and the Class members' personal and financial information from theft, collection and misuse by third parties.

88. Marriott further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiffs and the Class of the security breach.

89. Plaintiffs' and Class members' PII was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated without their authorization as the direct and proximate result of Marriott's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class members' PII.

90. The policy of preventing future harm further weighs in favor of finding a special relationship between Marriott and the Class. Consumers count on Marriott to keep their personal information safe. If companies are not held accountable for failing to take reasonable security measures to protect consumers' private and personal information, such as names, social security

numbers, and contact information, they will not take the steps that are necessary to protect against future data breaches.

91. It was foreseeable that if Marriott did not take reasonable security measures, the data of Plaintiffs and members of the Class would be taken.

92. Major hotels like Marriott face a higher threat of security breaches than other types and sizes of businesses due in part to the scope and breadth of the personal, private, and sensitive information that hoteliers, including Marriott possesses about hundreds of millions of consumers.

93. As a direct and proximate result of Marriott's conduct and breach of its duties, Plaintiffs and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (v) failure to receive the full benefit of their bargain as a result of receiving hotel accommodation services that were less valuable than what they paid for.

94. Neither Plaintiffs nor other members of the Class contributed to the security breach, nor did they contribute to Marriott's employment of insufficient security measures to safeguard consumers' PII, including passport numbers and debit and credit card information.

95. Plaintiffs and the Class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

96. Marriott's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach constitute common law negligence, gross negligence, and negligence *per se*.

SECOND CAUSE OF ACTION

Violations of the California Customer Records Act (Civil Code §§ 1798.80, *et seq*.)

97. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

98. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act (the "California CRA"), Civil Code § 1798.81.5, which requires that any business that "owns licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

99. The events alleged herein constituted a "breach of the security system" of Marriott within the meaning of Civil Code § 1798.82.

100. The information lost, disclosed, or intercepted during the events alleged herein constituted unencrypted "personal information" within the meaning of Civil Code §§ 1798.80(e) and 1798.82(h).

101. Marriott failed to implement and maintain reasonable or appropriate security procedures and practices to protect consumers' personal and financial information. On information and belief, Marriott failed to employ industry standard security measures, best practices or safeguards with respect to consumers' personal and financial information.

102. Marriott failed to disclose the breach of security of its system in the most expedient time possible and without unreasonable delay after it knew or reasonably believed that consumers' personal information had been compromised.

103. The breach of the personal information of millions of Marriott's consumers' records constituted a "breach of the security system" of Marriott pursuant to Civil Code § 1798.82(g).

104. By failing to implement reasonable measures to protect consumers' personal data it maintained, Marriott violated Civil Code § 1798.81.5.

105. In addition, by failing to promptly notify all affected consumers that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Marriott violated Civil Code § 1798.82 of the same title in a manner that would reach all affected consumers.

106. By violating Civil Code §§ 1798.81.5 and 1798.82, Marriott "may be enjoined" under Civil Code § 1798.84(e).

107. Accordingly, Plaintiffs request that the Court enter an injunction requiring Marriott to implement and maintain reasonable security procedures to protect consumers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Marriott, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Marriott's systems on a periodic basis; (2) ordering that Marriott engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Marriott audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Marriott, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that Marriott, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (6) ordering Marriott to meaningfully educate

its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Marriott customers must take to protect themselves.

108. Plaintiffs further request that the Court require Marriott to: (1) identify and notify all members of the Class who have not yet been informed of the Data Breach; and (2) to notify affected customers of any future data breaches by email and text within 24 hours of Marriott's discovery of a breach or possible breach, and by mail within 72 hours.

109. As a result of Marriott's violation of Civil Code §§ 1798.81, 1798.81.5, and 1798.82, Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (v) failure to receive the full benefit of their bargain as a result of receiving hotel accommodation services that were less valuable than what they paid for.

110. Plaintiffs, individually and on behalf of the members of the Class, seeks all remedies available under Civil Code § 1798.84, including, but not limited to: (a) damages suffered by members of the Class; and (b) equitable relief. Plaintiffs, individually and on behalf of the members of the Class, also seek reasonable attorneys' fees and costs under applicable law.

THIRD CAUSE OF ACTION

Violations of the California Unfair Competition Law (Bus. & Prof. Code §§ 17200, *et seq.*)

111. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

112. The California Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of its above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Marriott engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

113. In the course of conducting its business, Marriott committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class members' PII, and violating the statutory and common law alleged herein in the process, including, *inter alia*, California's Customer Records Act (Civ. Code §§ 1798.80, *et seq.*), California's UCL, California's CLRA, and common law negligence. Plaintiffs and Class members reserve the right to allege other violations of law by Marriott constituting other unlawful business acts or practices. Marriott's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

114. Marriott also violated the UCL by failing to timely notify Plaintiffs and Class members regarding the unauthorized release and disclosure of their PII.

115. Marriott's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Marriott's wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. California has a well-defined public policy embodied by various states statutes,

including California's Customer Records Act and Information Practices Act to ensure that businesses that maintain customer's personal information implement and maintain reasonable security procedures and practices to protect the personal information from unauthorized access, destruction, use, modification or disclosure. The gravity of Marriott's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Marriott's legitimate business interests other than engaging in the above-described wrongful conduct.

116. The UCL also prohibits any "fraudulent business act or practice." Marriott's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

117. As a direct and proximate result of Marriott's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, and/or (v) failure to receive the full benefit of their bargain as a result of receiving hotel accommodation services that were less valuable than what they paid for.

118. Unless restrained and enjoined, Marriott will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class members, and the general public, also seeks restitution and an injunction prohibiting Marriott from continuing such wrongful conduct, and requiring Marriott to modify its corporate

culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

FOURTH CAUSE OF ACTION

Violations of the Consumers Legal Remedies Act (Civil Code §§ 1750, *et seq.*)

119. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

120. This cause of action is brought pursuant to the Consumers Legal Remedies Act, California Civil Code §§ 1750, *et seq*. (the "Act") and similar laws in other states. Plaintiffs are consumers as defined by California Civil Code § 1761(d). Marriott's hotel accommodations are a "good" within the meaning of the Act.

121. Marriott violated and continues to violate the Act by engaging in the following practices proscribed by California Civil Code § 1770(a)(19) ("Inserting an unconscionable provision in the contract") in transactions with Plaintiffs and the Class which were intended to result in, and did result in, the sale of its hotel accommodations.

122. Marriott violated the Act by inserting an unconscionable provision in the contract for the hotel accommodations it offers Plaintiffs, Class members and other consumers through the Data Breach. Buried within the fine-print adhesionary "Terms of Use" that accompany the hotel accommodations (and all goods offered by Marriott) are purportedly mandatory waivers of class actions against Marriott as well as any right to have a jury trial. Members of the Class also do not reasonably know that they are potentially giving up valuable legal rights by accepting Marriott's post-breach offer of the WebWatcher monitoring

product. On the other hand, Marriott, the drafter of the adhesionary provision and the party with superior bargaining power, receives unfairly one-sided benefits.

123. Pursuant to California Civil Code § 1782(d), Plaintiffs, individually and on behalf of the other members of the Class, seek a Court order enjoining the above-described wrongful acts and practices of Marriott and for restitution and disgorgement.

124. Pursuant to § 1782 of the Act, Plaintiffs notified Marriott in writing by certified mail of the particular violations of § 1770 of the Act, and demanded that Marriott rectify the problems associated with the actions detailed above and give notice to all affected consumers of Marriott's intent to so act. A copy of the letter is attached hereto as Exhibit A.

125. If Marriott fails to rectify or agree to rectify the problems associated with the actions detailed above and give notice to all affected consumers within 30 days of the date of written notice pursuant to § 1782 of the Act, Plaintiffs will amend this complaint to add claims for actual, punitive and statutory damages, as appropriate.

126. Marriott's conduct is fraudulent, wanton, and malicious.

127. Pursuant to § 1780(d) of the Act, attached hereto as Exhibit B is the affidavit showing that this action has been commenced in the proper forum.

SIXTH CAUSE OF ACTION

Violation of the Florida Deceptive and Unfair Trade Practices Act Florida Stat. §§ 501.201, *et seq*.

128. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

129. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*. ("FDUTPA"). The stated purpose of the FDUTPA is to "protect the consuming public … from those who engage in unfair methods of competition, or unconscionable,

deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

130. Plaintiff Johnson and Florida Class members are "consumers" as defined by Fla. Stat. § 501.203.

131. Marriott advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida within the meaning of the FDUTPA.

132. Florida Statute § 501.204(1) declares unlawful "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce."

133. Florida Statute § 501.204(2) states that "due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to [section] 5(a)(1) of the Federal Trade Commission Act." Defendant's unfair and deceptive practices are likely to mislead – and have misled – the consumer acting reasonably in the circumstances, and violate Fla. Stat. § 500.04 and 21 U.S.C. § 343.

134. Defendant has violated the FDUTPA by engaging in the unfair and deceptive practices as described herein which offend public policies and are immoral, unethical, unscrupulous and substantially injurious to consumers.

135. Plaintiffs and the Class have been aggrieved by Defendant's unfair and deceptive practices and acts of failing to safeguard Plaintiffs' and Class members' PII, and by inserting an unconscionable provision in the contract for the hotel accommodations it offers Plaintiffs, Class members and other consumers through the Data Breach and its sale of goods. Buried within the fine-print adhesionary "Terms of Use" that accompany the hotel accommodations (and all goods offered by Marriott) are purportedly mandatory waivers of class actions against Marriott as well as any right to have a jury trial. Members of the Class also do not reasonably know that they are potentially

giving up valuable legal rights by accepting Marriott's post-breach offer of the WebWatcher monitoring product. On the other hand, Marriott, the drafter of the adhesionary provision and the party with superior bargaining power, receives unfairly one-sided benefits.

136. Marriott also violated the FDUTPA by failing to timely notify Plaintiffs and Class members regarding the unauthorized release and disclosure of their PII.

137. The harm suffered by Plaintiffs and the Class were directly and proximately caused by the deceptive, misleading and unfair practices of Defendant, as more fully described herein.

138. Pursuant to Fla. Stat. § 501.211(1), Plaintiffs and the Class seek an order for restitution, disgorgement, and damages.

139. Additionally, pursuant to Fla. Stat. §§ 501.211(2) and 501.2105, Plaintiffs and the Class make claims for damages, attorneys' fees and costs.

FIFTH CAUSE OF ACTION

Declaratory Relief

140. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

141. An actual controversy has arisen in the wake of the Data Breach regarding Marriott's duties to safeguard and protect Plaintiffs' and Class members' confidential and sensitive PII. Marriott's PII security measures were (and continue to be) woefully inadequate. Marriott disputes these contentions and contends that its security measures are appropriate.

142. Plaintiffs and Class members continue to suffer damages, other injury or harm as additional identity and financial theft and fraud occurs.

143. Therefore, Plaintiffs and Class members request a judicial determination of their rights and duties, and ask the Court to enter a judgment declaring, *inter alia*, (i) Marriott owed (and continues to owe) a legal duty to

safeguard and protect Plaintiff's and Class members' confidential and sensitive PII, and timely notify them about the Data Breach, (ii) Marriott breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class members' confidential and sensitive PII, and (iii) Marriott's breach of its legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiffs and Class members. A declaration from the Court ordering Marriott to stop its illegal practices is required. Plaintiffs and Class members will otherwise continue to suffer harm as alleged above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all persons and consumers similarly situated, prays for judgment as follows:

A. An Order certifying the proposed Class defined herein, designating Plaintiffs as representatives of said Class, and appointing the undersigned counsel as Class Counsel;

B. For restitution of all amounts obtained by Marriott as a result of its wrongful conduct in an amount according to proof at trial, plus pre-judgment and post-judgment interest thereon;

C. For all recoverable compensatory, consequential, actual, and/or statutory damages in the maximum amount permitted by law;

D. For punitive and exemplary damages;

E. For other equitable relief;

F. For such injunctive relief, declaratory relief, orders, or judgment as necessary or appropriate to prevent these acts and practices;

G. For payment of attorneys' fees and costs of suit as allowable by law; and

H. For all such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all issues so triable.

Respectfully submitted,

Dated: December 18, 2018

BLOOD HURST & O'REARDON, LLP
LESLIE E. HURST (178432)
PAULA R. BROWN (254142)

By: *s/ Leslie E. Hurst*
LESLIE E. HURST

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
lhurst@bholaw.com
pbrown@bholaw.com

ERNST LAW GROUP
MATTHEW TAYLOR ERNST (277901)
1020 Palm Street
San Luis Obispo, CA 93401
Tel: 805/541-0300
805/541-5168 (fax)
TE@ErnstLawGroup.com

Attorneys for Plaintiff